Set Task Electronic Template – Unit 11

Task B - Activity 4 Template: Forensic Incident Analysis

*Use the section headings below to structure a response for **each** evidence item.*

Evidence item: 1. Baljinder's account

Method of acquiring the evidence:
Baljinder's recollection of the event.
Evidence detail:
The items couldn't be found after one of the items (Laptop) was booked to be used and it couldn't be found. The other items were realised to be missing as they began to search for the laptop. Baljinder's recollection give an estimated timeline of the event.
Evidence reliability:
Good. Baljinder is responsible for the network and the security matters, meaning he will take a professional approach to the event.
Conclusions:
It was a mistake to leave the phone and laptop charging on the table. There should be an equipment list done at the end of every day, this would help pinpoint the exact time when the USBs, Mice and keyboards were taken. They were correct not to take out a claim on the Laptop and phone, due to the age.

Evidence item: 2. summary of a meeting with the EH management company

Method of acquiring the evidence:
Notes taken from the meeting with Edexcelsior House. Baljinder summarised the main points taken from the meeting.
Evidence detail:
The meeting identified a number of disturbances that occurred in the building during the weekend. The meeting removed the any clearers from the equation, as they are loyal and there hasn't been any dishonesty cases this year. There were a number of thefts reported on Friday but were less present for the rest of the weekend. There was no evidence of forced entry to any of the floor which got robbed. The shops had reports of phantom charges applied to contactless payments. These charges has happened before due to system errors, however there were no reports of errors over the weekend.
Evidence reliability:
Good. Baljinder took the key points from the meeting, however there is a chance that some details may have been missed.
Conclusions:
It is clear that there were a number of people around whom intended on stealing from the building during the weekend. The phantom charges may be the most important point to come from the meeting, as it is likely that this has something to do with the point of entry for the theft to occur. Although the meeting seemed to rule out any foul play from the cleaners, there is still a possibility it could be one of them.

Evidence item: 3. door access control logs

Method of acquiring the evidence:
The log is automatically created by the system, it is controlled and supplied by EH management company.

Evidence detail:
The log shows who had access, where they accessed and when they did so. The log shows that there were a number of cleaners and security guards who entered and exited the floor, all of these are accounted for. There are three failed attempts to gain enter the floor and one successful entrance to the floor, all in close succession of each other.
Evidence reliability:
Good. The logs are produced by a specific software designed for this purpose.
Conclusions:
The log displays quite normal activity for the most part of it. However, it does also show some potential suspicious activity on the Saturday night, at 23:31-23:32. The three failed attempts to enter the floor may be attempts from attackers/thief's, the final attempt shows a successful attempt to gain access. The times at which these attempts were made are very close to one another, if these were legitimate attempts, you would think that they would have seen each other. However, nothing was mentioned in the notes, which makes me believe it to be foul play/when the theft occurred.

Evidence item: 4. network diagram

Method of acquiring the evidence: Documentation that would have been made when the network was first set up.
Evidence detail: The diagram shows how the Main Switch is the main component of the network, this is because each component connects to it. There are no connections between individual components, on single connections to the Main Switch.
Evidence reliability: Good. There is nothing that suggests that the layout has been changed.
Conclusions: The diagram shows us all the possibilities that an attacker could use in order to gain access to the floor. It is apparent that the main switch has the most important role in the network and it is a possibility that is how the thief's managed to gain access. There is a possibility that the thief's used a Wi-Fi connection to attack and gain control to the Electronic door control system. However, this situation is less likely to happen, as the information that was gathered in tasks 2&3 suggests an alternative form of access to the floor.

Evidence item: 5. laptop tracking report

Method of acquiring the evidence:
An application that enables users to identify the location of their device, depending on the last time it connected to the internet. Although not perfect, Windows10 'Find my Device' is quite accurate.
Evidence detail:
The devices location is in Nairobi, Kenya. There was only one connection made on 09/04/2018, which was six days after the activation of 'Find My Device'.
Evidence reliability:
Fair. The device can only be tracked when it is connected to the Wi-Fi, without an internet connect the application is useless.
Conclusions:
Although the location of the device has been identified, the evidence doesn’t identify how the laptop got there. There can be no definite link made to any other of the evidences provided. A unusual thing is that 'Find My Device' wasn’t already switched on, if it was they would have been able to track the laptop straight away.

Final Conclusion
The missing items from the 19th floor could have been taken in a number of different ways.

Given the evidence which was presented, I believe the most likely explanation is that the employee cards were either stolen or manipulated in some way. There is a link between the phantom card charges and the access to the floor. A likely situation is that the thieves used the contactless card technology to get the information of employee cards. Once collecting the cards, they then proceeded to go to the 19th floor and try different employee cards unit one of them worked, giving them access. Once inside, the thieves grabbed what they could easily get, the laptop and phone left on the table and various appliances from systems. The thieves then exited the floor using the push button that unlocks the doors from the inside. I believe that this is the most likely explanation as the information given by the employees, whose cards were involved, all places them at a different location to where the theft went down. As well as the reports to the phantom card charges and thefts which occurred the day before the incident.

A less likely explanation is that the electrical appliances were stolen by either the cleaners or security team. This may have occurred anyone of the times they logged into the floor, while doing their job. However, in the meeting which Baljinder attended, it was made clear that the employees are employed directly from EH and they have better pay and working conditions compared to similar jobs in the area.

The least likely explanation is that attackers were able to manipulate the Main Switch on the floor to gain access to the doors. The attackers may have been able to hack the main switch while using a device connected to the Wi-Fi. I feel this is the least likely explanation, as the software needed to complete this task is very complicated, and the items that were stolen don’t seem to be worth the time or effort.